Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane

Jean-Charles Faugère, Jules Svartz

Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane

Jean-Charles Faugère, Jules Svartz
INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy-Kennedy
Case 169, 4, Place Jussieu, F-75252 Paris
{Jean-Charles.Faugere,Jules.Svartz}@lip6.fr

ABSTRACT

We propose an efficient algorithm to solve polynomial systems of which equations are *globally* invariant under an action of the symmetric group $\mathfrak{S}_N$ acting on the variable x_i with $\sigma(x_i) = x_{\sigma(i)}$ and the number of variables is a multiple of N. For instance, we can assume that swapping two variables (or two pairs of variables) in one equation gives rise to another equation of the system (perhaps changing the sign). The idea is to apply many times divided difference operators to the original system in order to obtain a new system of equations involving only the symmetric functions of a subset of the variables. The next step is to solve the system using Gröbner techniques; this is usually several order faster than computing the Gröbner basis of the original system since the number of solutions of the corresponding ideal, which is always finite has been divided by at least $N!$.

To illustrate the algorithm and to demonstrate its efficiency, we apply the method to a well known physical problem called equilibria positions of vortices. This problem has been studied for almost 150 years and goes back to works by von Helmholtz and Lord Kelvin. Assuming that all vortices have same vorticity, the problem can be reformulated as a system of polynomial equations invariant under an action of $\mathfrak{S}_N$. Using numerical methods, physicists have been able to compute solutions up to $N \leq 7$ but it was an open challenge to check whether the set of solution is complete. Direct naive approach of Gröbner bases techniques give rise to hard-to-solve polynomial system: for instance, when $N = 5$, it takes several days to compute the Gröbner basis and the number of solutions is 2060. By contrast, applying the new algorithm to the same problem gives rise to a system of 17 solutions that can be solved in less than 0.1 sec. Moreover, we are able to compute *all* equilibria when $N \leq 7$.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

1. INTRODUCTION

Solving general polynomial systems is a fundamental problem in Computer Algebra. However it must be emphasized that polynomial systems arising in applications are very often highly structured. For instance, in several algebraic problems coming from applications the solutions (the algebraic variety) is invariant under the action of a finite group: for example the Cyclic-n problem [10], in Cryptography the NTRU Cryptosystem [12] or the membrane inclusions curvature equations in biology [6]. Hence an important subproblem is to solve efficiently such algebraic problems. We should consider two distinct cases. First, if all the equations are invariant under the action of the group, there are two ways to solve the system using the symmetries. In [3] Colin propose to use invariants [17] to solve the system. This method is very efficient if the Hironaka Decomposition of the ring of invariants is simple, but for the Cyclic-n problem, for example, it seems better to use a second method based on SAGBI Gröbner Basis techniques [8]. The second class of problems, which is probably the most important in practice, is to consider polynomial systems of which the set of solutions is globally invariant under the action of a finite group (this is the case of the biology example [6]). The goal of the present paper is to propose an efficient method to solve such problems assuming that the group is the whole symmetric group. To illustrate the algorithm and to demonstrate its efficiency, we apply the method to a well known physical problem called equilibria positions of vortices.

The problem of finding and classifying all relative equilibria of N-point vortices in the plane is of long-standing interest. In the plane, attacks on the problem date back to the 1800s with the works of von Helmholtz [11] and later in the works by Thomson [14] (the later Lord Kelvin). A complete bibliography of papers on the subject can be found in [16] or [2]. Several families of equilibria have been found [2] and other solutions have been found numerically, see [5]. More generally, the problem of equilibria on manifolds with different potentials has been studied by Albouy [1].

In the planar case, the problem is equivalent to solve the following algebraic system (in the following Z symbolizes the complex conjugate of z): $Z_i = \sum_{j=1, j\neq i}^{N} \frac{1}{z_i - z_j}$. In this paper we describe a general algorithm and for each step we apply it to the equilibria of N-point vortices. The proposed algorithms is a 3 steps process:

1. We apply many times divided difference operators (see sec-

tion 3) to the original system in order to obtain a new system of equations involving only invariant equations. For instance, the $4-$vortex problem is equivalent to $r_0 = s_1 = r_1 - 6 = r_2 = 2r_3 + 5s_2 = 0$ where $r_k = \sum_i Z_i z_i^k$ and $s_k = \sum_i z_i^k$ is the Newton sum.

2. As explained in section 4, the second step is to eliminate all the variables but the z_i. For that purpose, we require that the algebraic system fulfils the parameterization assumption (see definition 6). We derive a new system of equations involving only the symmetric functions of a subset of the variables. For instance, for the 4-vortex problem we obtain the symmetric system $e_3(e_2^2+12e_4)^2 = e_2(e_2^4 - 16e_2^2e_4 + 9e_2e_3^2 + 48e_4^2) = 0$.

3. The last step consists simply in solving the symmetric equations using standard Gröbner bases techniques.

The first step can be viewed as generalisation of [6], we give algorithms to obtain invariant equations under the action of $\mathfrak{S}_N$ on several blocks of variables.

Applied to the vortex problem, our method has three advantages over previous method:

1. In theory, it is possible to solve directly the original equations. However, when $N = 5$, it take several days to compute the Gröbner basis and the number of solutions is 2060. By contrast, applying the new algorithm to the same problem give rise to a system of 17 solutions that can be solved in less than 0.1 sec. The case $N = 7$ can be completely solved in about 20 minutes.

2. We are sure to find all the solutions, so we give a certificate for the previous numerical solutions. For $N \geq 5$, it is completely new.

3. Two distinct solutions could be so close, that 300 digits are needed to be sure that they are distinct, see [5] for example. With exact computations, the solutions appear to be distinct without further computations.

Since we are using only exact computations, our algorithms gives computational proofs of the solutions of the vortex problem.

2. VORTEX PROBLEM

2.1 Physical equations and first steps

We start with the equations of motion for the N body problem:

$$\frac{\partial^2}{\partial t^2}\mathbf{r}_i = \sum_{j\neq i} m_j U'(s_{ij})(\mathbf{r}_i - \mathbf{r}_j) \text{ for } i = 1,\ldots,N \qquad (1)$$

where m_i and $\mathbf{r}_i$, are, respectively the mass and the position vector (relative to the center of mass) for the i-th particle and $s_{ij} = |\mathbf{r}_i - \mathbf{r}_j|^2$ is the square of the distance between particle i and j; $U(s)$ is the potential function such that $U'(s) = s^a$ for some real value. Without lost of generality we can assume that the center of mass is at the origin. Usually the potential is one of the two well known potential:

	a	*potential*
Newton	$-3/2$	$U(r) = r^{-\frac{1}{2}}$
Vortex	-1	$U(r) = \log(r)$

In this paper we assume that: we are in the planar case, all the masses (vortices) are equal (that is to say $m_i = 1$) and that the potential is the logarithmic one.

A central configuration is a configuration of bodies such that the acceleration vector for each body is a common scalar multiple of its position vector:

$$\frac{\partial^2}{\partial t^2}\mathbf{r}_i = \lambda \mathbf{r}_i \text{ where } \lambda \text{ is real} \geqslant 0 \qquad (2)$$

Central configurations are of interest for a variety of reasons: To every central configuration is corresponding a homothetic solution – a solution which retains its shape for all time, while expanding, contracting and rotating about the center of mass.

We identify the real plane $\mathbb{R}^2$ with the complex plane $\mathbb{C}$. As we will see, in the planar case, it is easier to work with complex positions $z_i = x_i + \imath y_i = \mathbf{r}_i$. Hence $s_{i,j} = |\mathbf{r}_i - \mathbf{r}_j|^2 = (z_i - z_j)(\bar{z}_i - \bar{z}_j)$ where $\bar{z}$ is the complex conjugate of z. Combining (1) and (2) we obtain:

$$\lambda z_i = \sum_{j\neq i} \frac{(z_i - z_j)}{(z_i - z_j)(\bar{z}_i - \bar{z}_j)} = \sum_{j\neq i} \frac{1}{\bar{z}_i - \bar{z}_j} \qquad (3)$$

By summing over the i, we see that $\sum z_i = 0$ (the center of mass is at the origin), so e_1, the first symmetric function of the z_i, is equal to zero. Moreover, since $\lambda > 0$, we observe that the conjugate of equation (3) is equivalent to:

$$\sqrt{\lambda}\bar{z}_i = \sum_{j=1, j\neq i}^{N} \frac{1}{\sqrt{\lambda}z_i - \sqrt{\lambda}z_j}$$

Therefore, we can suppose $\lambda = 1$ and recover the original solutions by multiplying the solutions of the case $\lambda = 1$ by $\sqrt{\lambda}$. Knowing z_i, it is easy to recover λ using the following property

Proposition 1 $2\lambda \sum_{i=1}^N |z_i|^2 = N(N-1)$

PROOF. $\lambda \sum_{i=1}^N z_i\bar{z}_i = \sum_{i=1}^N \sum_{j=1, j\neq i}^N \frac{z_i}{z_i - z_j} = \sum_{i=1}^N \sum_{j=1, j\neq i}^N (1 + \frac{z_j}{z_i - z_j})$ and thus $\lambda \sum_{i=1}^N z_i\bar{z}_i = N(N-1) - \lambda \sum_{j=1}^N z_j\bar{z}_j$ □

In summary, the central configuration problem is equivalent to:

$$\bar{z}_i = \sum_{j=1, j\neq i}^{N} \frac{1}{z_i - z_j} \qquad (E_i)$$

2.2 Symmetries of the solutions

2.2.1 *Action of* $\mathfrak{S}_N$

The permutation group $\mathfrak{S}_N$ acts on the variables $\{z_1,\ldots,z_N\}$ with $\sigma(z_i) = z_{\sigma(i)}$, and σ sends the equation (E_i) on the equation $E_{\sigma(i)}$. So, if $(z_1,\ldots,z_N)$ is a solution of the problem, any of the $N!$ N-uples $(z_{\sigma(1)},\ldots,z_{\sigma(N)})$ is still a solution.

2.2.2 *Action of* $\mathscr{O}_2(\mathbb{R})$

The isometry group of $\mathbb{R}^2$ can be identified to a transformation group on $\mathbb{C}$ generated by the rotations $z \mapsto az$ with a a complex of modulus one, and the symmetry $z \mapsto \bar{z}$. These transformations act on $\mathbb{C}^N$ by $(z_1,\ldots,z_N) \mapsto (az_1,\ldots,az_N)$ and $(z_1,\ldots,z_N) \mapsto (\bar{z_1},\ldots,\bar{z_N})$. If we multiply (E_i) by $\bar{a}$ or if we conjugate (E_i), we see that the set of solutions is invariant under this action.

Consequently, the set of solutions is invariant under the action of $\mathfrak{S}_N \times \mathscr{O}_2(\mathbb{R})$. We will first focus on the action of $\mathfrak{S}_N$ to obtain invariant equations, and finally use the action of $\mathscr{O}_2(\mathbb{R})$ to speed up the Gröbner Basis computation (see section 5).

2.3 Algebraic reformulation

Algebraically, it is impossible to separate $\imath$ and $-\imath$, and therefore z and $\bar{z}$. Thus, we introduce N new variables $Z_1,\ldots,Z_N$ that represent $\bar{z}_1,\ldots,\bar{z}_N$. The algebraic relations between these $2N$ variables are :

$$Z_i = \sum_{j\neq i} \frac{1}{z_i - z_j} \quad \text{and} \quad z_i = \sum_{j\neq i} \frac{1}{Z_i - Z_j} \qquad (E_i, \bar{E}_i)$$

To obtain polynomials, we multiply the equation E_i by $D_i = \prod_{j\neq i}(z_i - z_j)$ to obtain the polynomial equation $U_i = 0$ where

$$U_i = Z_i \prod_{j\neq i}(z_i - z_j) - \sum_{j\neq i\, k\neq i,j} \prod (z_i - z_k) \in \mathbb{Q}[z_1, \ldots, z_N, Z_1, \ldots, Z_N]$$

Remark 1 *Observe that permuting z_i and Z_i for all i transforms the equation (E_i) in $(\bar{E}_i)$, because of complex conjugation. Thus, for every relation in the ideal generated by the $2N$ equations $(E_i, \bar{E}_i)$ in $\mathbb{Q}[z_1, \ldots, z_N, Z_1, \ldots, Z_n]$, there is another one obtained by permuting z_i and Z_i.*

The following lemma is useful to express the equations $(E_i, \bar{E}_i)$ in a very compact way.

Lemma 1 *All the solutions of the vortex problem satisfy the following rational equations:*

$$Z_i = \frac{1}{2} \frac{Q''(z_i)}{Q'(z_i)} \tag{4}$$

where $Q(z) = \prod_{i=1}^{N}(z - z_i) = z^N + e_2 z^{N-2} + \cdots + (-1)^N e_N$ (recall that $e_1 = 0$), where e_i is the i-th elementary symmetric function of the z_i.

PROOF. Let $Q_i(z) = \frac{Q(z)}{z - z_i} = \prod_{j\neq i}(z - z_j)$, then $\frac{Q_i'(z)}{Q_i(z)} = \sum_{j\neq i} \frac{1}{z - z_j}$, so that $\frac{Q_i'(z_i)}{Q_i(z_i)} = Z_i$ according to equation (E_i). But we can write $Q(z) = (z - z_i)Q_i(z)$, and with two derivations, we obtain $Q'(z) = Q_i(z) + (z - z_i)Q_i'(z)$ and $Q''(z) = 2Q_i'(z) + (z - z_i)Q_i''(z)$. Setting $z = z_i$, we have $Q_i(z_i) = Q'(z_i)$ and $Q''(z_i) = 2\,Q_i'(z_i)$ so that we get the proof of the lemma. □

$\mathfrak{S}_N$ acts on $\{1, \ldots, N\}$, and therefore on $\{z_1, \ldots, z_N, Z_1, \ldots, Z_N\}$.

The next step is to obtain equations depending only of the e_i, the symmetric functions of the z_i. In the next section we will see how to obtain equations of lower degree individually invariant under $\mathfrak{S}_N$.

3. FROM INVARIANT SYSTEM TO INVARIANT EQUATIONS

In this section, we will generalize the previous situation with more than two blocks of variables. More precisely we assume that we have to solve the following polynomial system:

$$U_i = 0 \text{ for } i = 1, \ldots, N$$

where each equation U_i is a polynomial in $\mathbb{A}[\mathscr{Z}, \mathscr{V}]$ where $\mathbb{A}$ is an integral domain (for instance, a polynomial ring with coefficients in $\mathbb{K}$), $\mathscr{Z}$ is the set $\{z_1, \ldots, z_N\}$ and $\mathscr{V}$ is another set of variables. We assume that $\mathfrak{S}_N$ acts on $\mathscr{Z} \cup \mathscr{V}$.

3.1 Invariant system under $\mathfrak{S}_N$

We suppose that $|\mathscr{V}|$ is a multiple of N, and that $\mathfrak{S}_N$ acts on each block of N variables like it acts on $\mathscr{Z}$ such that $\sigma(z_i) = z_{\sigma(i)}$. In fact, the product $\mathfrak{S}_N \times \cdots \times \mathfrak{S}_N$ acts on the variables $\mathscr{Z} \cup \mathscr{V}$. Let $\{(U_i)\}$ be a system of N equations, which is globally invariant under the subgroup of $\mathfrak{S}_N \times \cdots \times \mathfrak{S}_N$ of which elements are of the form $\sigma \times \cdots \times \sigma$: that means that for every $\tilde{\sigma} = \sigma \times \cdots \times \sigma$ and every i, it exists j such that $\tilde{\sigma}.U_i = U_j$.

Remark 2 *We could introduce the ring of invariants of this subgroup, but its Hironaka Decomposition [17] is not simple enough to allow easy computations.*

We want to obtain from the original set of equations $\{U_i\}$ a new set of equations $\{V_i\}$ which are individually invariant under the action of $\mathfrak{S}_N$, which means that for all i and $\tilde{\sigma}$, $\tilde{\sigma}.V_i = V_i$. To this end, we will use divided differences.

3.2 Divided differences on one block

Here, we first assume that we only have one block of variables $\mathscr{Z} = \{z_1, \ldots, z_N\}$, $\mathscr{V} = \emptyset$ and N equations $U_i \in \mathbb{A}[z_1, \ldots, z_N]$ such that $\sigma(U_i) = U_{\sigma(i)}$ for all σ in $\mathfrak{S}_N$.

Definition 1 *Given $U_1, \ldots, U_N$ we define recursively the divided differences by:*

$$[U_i] = U_i \quad \textit{for} \quad i = 1, \ldots, N$$
$$[U_{i_1}, \cdots, U_{i_k}] = \frac{[U_{i_1}, \cdots, U_{i_{k-1}}] - [U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}]}{z_{i_{k-1}} - z_{i_k}}$$

for any given distinct integers $\{i_1, \ldots, i_k\}$ in $\{1, \ldots, N\}$.

Theorem 1 *The divided difference $[U_{i_1}, \cdots, U_{i_k}]$ is a polynomial in $\mathscr{Z}$ and depends only on the set $\{i_1, \ldots, i_k\}$, so for any subset $\mathscr{P} = \{i_1, \ldots, i_k\}$, we set $[U]_{\mathscr{P}} = [U_{i_1}, \ldots, U_{i_k}]$. Moreover, for any subset $\mathscr{P}$ of $\{1, \ldots, N\}$, and for any σ in $\mathfrak{S}_N$, $\sigma([U]_{\mathscr{P}}) = [U]_{\sigma(\mathscr{P})}$.*

PROOF. We prove the first part by induction on $k \in \{1 \ldots, N\}$. For $k = 1$ it is obvious. Suppose the theorem is true for $k - 1$, and let $\{i_1, \ldots, i_k\}$ be like in the statement.
Let $\tilde{\mathbb{A}} = \mathbb{A}[z_1, \ldots, z_{i_{k-1}-1}, z_{i_{k-1}+1}, \ldots, z_N]$. Since $z_{i_{k-1}} - z_{i_k}$ is monic as polynomial in $\tilde{\mathbb{A}}[z_{i_{k-1}}]$, we can perform the division of $[U_{i_1}, \cdots, U_{i_{k-1}}] - [U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}]$ by $z_{i_{k-1}} - z_{i_k}$, and by sending $z_{i_{k-1}}$ on z_{i_k}, we see that the rest is equal to 0, so $[U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}]$ belongs to $\mathbb{A}[\mathscr{Z}]$. Moreover, by acting on the equality $[U_{i_1}, \cdots, U_{i_k}](z_{i_{k-1}} - z_{i_k}) = [U_{i_1}, \cdots, U_{i_{k-1}}] - [U_{i_1}, \cdots, U_{i_{k-2}}, U_{i_k}]$ with any permutation σ, we deduce the second part again by induction on N. □

It is usual to introduce a special notation in the case of univariate polynomials:

Definition 2 *Let $\mathbb{K}$ be a field, and $F(z)$ an univariate polynomial in $\mathbb{K}[z]$. We define $F(z_1, \ldots, z_N) = [F(z_1), \ldots, F(z_N)]$.*

The two following lemmas will be useful later.

Lemma 2 *For an univariate polynomial $F(z) \in \mathbb{K}[z]$ we have $F(z_1, \ldots, z_N) = \sum_{i=1}^{N} \frac{F(z_i)}{Q'(z_i)}$ where $Q(z) = \prod_{i=1}^{N}(z - z_i)$.*

PROOF. We prove this by induction on N. For $N = 1, Q(z) = (z - z_1)$ so the assertion is obvious. Suppose that we have proved this lemma for $N - 1$. Let $U(z) = \prod_{i=1}^{N-1}(z - z_i)$ and $V(z) = \prod_{i=1}^{N-2}(z - z_i) \times (z - z_N)$. Hence, $Q(z) = U(z)(z - z_N) = V(z)(z - z_{N-1})$ which implies that $Q'(z) = U(z) + U'(z)(z - z_N) = V(z) + V'(z)(z - z_{N-1})$. Consequently,
$F(z_1, \ldots, z_N) = \frac{\frac{F(z_1)}{U'(z_1)} + \frac{F(z_N)}{V'(z_N)} + \sum_{i=2}^{N-1} \frac{F(z_i)}{U'(z_i)} + \frac{F(z_i)}{V'(z_i)}}{z_{N-1} - z_N} = \sum_{k=1}^{N} \frac{F(z_k)}{Q'(z_k)}$, and the lemma is proved. □

Definition 3 *For $\mathscr{Z} = \{z_1, \ldots, z_N\}$, we define h_k the k-th symmetric complete function as the sum of all monomials of degree k on the variables in $\mathscr{Z}$. By extension, $h_k = 0$ when $k < 0$ and $h_0 = 1$.*

Lemma 3 *For any k, if $F(z) = z^k$, then $F(z_1, \ldots, z_N) = h_{k-N+1}$.*

PROOF. We prove this by induction on N as well. If $N = 1$, $F(z_1) = z_1^k$ is the complete symmetric function of degree k on one variable z_1. For $N \geq 2$, $F(z_1, \ldots, z_N) = \frac{F(z_1, \ldots, z_{N-1}) - F(z_1, \ldots, z_{N-2}, z_N)}{z_{N-1} - z_N}$

By induction, $F(z_1,\dots,z_{N-1})-F(z_1,\dots,z_{N-2},z_N)=\sum(z_{N-1}^{k-N+2-u}-z_N^{k-N+2-u})\times m$, where the sum is all over the monomials m in $z_1,\dots,z_{N-2}$ of degree $u\in\{0,\dots,k-N+2\}$. Writing $z_{N-1}^{k-N+2-u}-z_N^{k-N+2-u}=(z_{N-1}-z_N)\sum m'$, where the sum is all over the monomials m' in z_{N-1},z_N of degree $k-N+1-u$, we obtain exactly the complete symmetric function in $z_1,\dots,z_N$ of degree $k-N+1$. □

3.3 Invariant equations

We explain here how to obtain invariant equations from divided differences in case of one block of variables.

Theorem 2 *Let V_i be $\sum_{\mathscr{P}\subset\{1,\dots,N\},|\mathscr{P}|=i}[U]_{\mathscr{P}}$ for all $i\in\{1,\dots,N\}$. We obtain N equations invariant under $\mathfrak{S}_N$, and the varieties associated respectively to $\{V_i\}$ and $\{U_i\}$ are the same, except maybe for points with two equal components.*

PROOF. Any σ in $\mathfrak{S}_N$ realizes a permutation of the subsets of $\{1,\dots,N\}$ with same cardinality, and also a permutation of the $[U]_{\mathscr{P}}$. Therefore, $\sigma(V_i)=V_i$ for all i in $\{1,\dots,N\}$. Suppose that $\underline{\alpha}=(\alpha_1,\dots,\alpha_N)$ is a common zero of the U_i, without equal components. Then, we deduce easily that all the $[U]_{\mathscr{P}}(\underline{\alpha})$ are equal to zero, and also the $V_i(\underline{\alpha})$. Conversely, if $V_N(\underline{\alpha})=0$ then all the $[U]_{\mathscr{P}}(\underline{\alpha})$ with $\mathscr{P}$ of cardinality $N-1$ are equal, because V_N can be written as $\frac{[U]_{\mathscr{P}}-[U]_{\mathscr{Q}}}{z_k-z_\ell}$ where $\mathscr{P}$ and $\mathscr{Q}$ are two distinct subsets of cardinality $N-1$, $z_k=\mathscr{P}\backslash\mathscr{Q}$ and $z_\ell=\mathscr{Q}\backslash\mathscr{P}$. But their sum $V_{N-1}(\underline{\alpha})$ is equal to zero, so they are equal to zero. We can repeat it for $N-2,N-3,\dots,1$ to deduce that $U_i(\underline{\alpha})=0$ for all i. □

Definition 4 *We define the Reynolds operator [4] on $\mathfrak{S}_N$ by*

$$\begin{array}{rccc}\mathfrak{R}: & \mathbb{A}[z_1,\dots,z_N] & \longrightarrow & \mathbb{A}[z_1,\dots,z_N]\\ & P & \mapsto & \frac{1}{N!}\sum_\sigma\sigma(P)\end{array}$$

Remark 3 *We just have to compute all the $[U_1,\dots,U_k]$ for k in $\{1,\dots,N\}$ to obtain the V_i, because $V_i=\binom{i}{N}\mathfrak{R}([U_1,\dots,U_i])$. We deduce from this fact a simple algorithm to compute the set $\{V_i\}$.*

Let $\tau_{i,j}$ be the transposition permuting i and j.

ComputeInvariantSystem

Input: Variables $\{z_1,\dots,z_N\}$ and the polynomials U_i.
Output: The polynomials $V_1,\dots,V_N$.

1. for $k=2$ **to** N **do**
$[U_1,\dots,U_k]:=\text{Quo}([U_1,\dots,U_{k-1}]-\tau_{k-1,k}([U_1,\dots,U_{k-1}]),z_{k-1}-z_k)$;
end for.

2. return $\{\binom{k}{N}\mathfrak{R}([U_1,\dots,U_k]),k=1\dots N\}$ where $\mathfrak{R}$ is the Reynolds operator.

Since $\mathbb{K}[z_1,\dots,z_N]^{\mathfrak{S}_N}=\mathbb{K}[e_1,\dots,e_N]$, we can reformulate the equations V_i in terms of the symmetric functions of the z_i. The goal is now to generalize this fact in the case of several blocks of variables.

3.4 Generalization to several blocks

Assume that the equations U_i involve the set $\mathscr{Z}=\{z_1,\dots,z_N\}$ and another set of variables $\mathscr{V}$ and that $\mathfrak{S}_N$ acts on $\mathscr{Z}\cup\mathscr{V}$. Assume that the U_i are equal to $D_iP_i+Q_i$, where $D_i=\prod_{j\neq i}(z_i-z_j)$, Q_i are polynomials in $\mathscr{Z}$, and for all σ, $\sigma(P_i)=P_{\sigma(i)}$ and $\sigma(Q_i)=Q_{\sigma(i)}$. The previous section corresponds to the case $P_i=0$, but when $P_i\neq 0$ we can still apply divided differences in the same way, and construct $[U_{i_1},\dots,U_{i_k}]$ for given distinct integers; we obtain a similar theorem :

Theorem 3 *(i) $[U_{i_1},\dots,U_{i_k}]$ is a polynomial in $\mathscr{Z}$ and $\mathscr{V}$ which depends only on the set $\{i_1,\dots,i_k\}$. Moreover for any σ and any $\mathscr{P}$, $\sigma([U]_{\mathscr{P}})=[U]_{\sigma(\mathscr{P})}$.*

(ii) $V_i=\sum_{|\mathscr{P}|=i}[U]_{\mathscr{P}}$ is invariant under the action of $\mathfrak{S}_N$ and the varieties associated to respectively V_i and U_i are the same, except maybe for points with two equal $\mathscr{Z}$-components.

Remark 4 *We can use the algorithm ComputeInvariantSystem to compute the V_i.*

3.5 Application to the vortex problem

We obtained this equation from the vortex problem :

$$U_i=Z_i\prod_{j\neq i}(z_i-z_j)-\sum_{j\neq i}\prod_{k\neq i,j}(z_i-z_k)$$

which can be written as $U_i=D_iP_i+Q_i$, with $P_i=Z_i$ and $Q_i=-\sum_{j\neq i}\prod_{k\neq i,j}(z_i-z_k)$. These polynomials verify $\sigma(P_i)=P_{\sigma(i)}$ and $\sigma(Q_i)=Q_{\sigma(i)}$.

Example 1 *For $N=3$, it is easy to compute the invariant polynomials V_1,V_2,V_3, and we obtain*

$$\begin{array}{ll}V_1=\sum_i Z_iz_i^2-\sum_{j\neq i}Z_iz_iz_j+\sum_{\{i,j,k\}=\{1,2,3\}}Z_iz_jz_k & \\ V_2=2\sum_i z_iz_i-\sum_{i\neq j}Z_iz_j-9 & V_3=\sum_i Z_i\end{array}$$

Using the equations $V_3=0$ and $\bar{V}_3=z_1+z_2+z_3=0$ in V_1 and V_2, we can rewrite the system as

$$V_1=4\sum_i Z_iz_i^2\qquad V_2=3\sum_i Z_iz_i-9\qquad V_3=0$$

Definition 5 *We introduce new invariants which will be very useful to reformulate the vortex problem in a very simple way:*

$$r_k=\sum_i Z_iz_i^k\quad\text{and}\quad R_k=\sum_i Z_i^kz_i$$

It is also useful to define the Newton sums:

$$s_k=\sum_i z_i^k\quad\text{and}\quad S_k=\sum_i Z_i^k$$

Example 2 *For $N=4$, after reformulation, we obtain:*

$$r_0=s_1=r_1-6=r_2=2r_3+5s_2=0$$

and the conjugate equations:

$$R_0=S_1=R_1-6=R_2=2R_3+5S_2=0$$

It turns out that, surprisingly, we can obtain a general and very simple expression of these equations for any N.

Theorem 4 (Invariant Equations) *For any N and k, the solution of the vortex problem satisfies the following invariant equations:*

$$2r_k=\sum_{i=0}^{k-1}s_is_{k-1-i}-ks_{k-1}\qquad\text{with } s_0=N. \tag{5}$$

To prove the theorem 4 we will first give a lemma.

Lemma 4 *For $N\in\mathbb{N}^\star$ and $k\in\mathbb{N}$, let e_k, h_k and s_k be respectively the symmetric functions, the complete symmetric functions, and the Newton sum of degree k in the variables $z_1,\dots,z_N$. (With the convention that $e_0=h_0=1$, $s_0=N$ and all these terms are zero when $k<0$ and e_k is zero for $k>N$). Then*

$$\sum_{j=0}^{N}(-1)^je_j(N-j)(N-j-1)h_{k-j-1}=\sum_{i=0}^{k-1}s_is_{k-1-i}-ks_{k-1}$$

PROOF. We introduce the series $E(t)=\sum e_k t^k=\prod_{i=1}^N(1+tz_i)$, $H(t)=\sum h_k t^k=\prod_{i=1}^N\frac{1}{1-tz_i}$ and $S(t)=\sum s_k t^k=\sum_{i=1}^N\frac{1}{1-tz_i}$. Let β_{k-1} and γ_{k-1} be the left and right terms of the equality we want to prove. We introduce $\beta(t)$ and $\gamma(t)$ the associated power series. Observe that $(N-j)(N-j-1)=N^2-N-2(N-1)j+j(j-1)$, so $\beta(t)=(N^2-N)E(-t)H(t)+2(N-1)tE'(-t)H(t)+t^2E''(-t)H(t)$ and $\gamma(t)=S^2(t)-S(t)-tS'(t)$. But $H(t)E(-t)=1$, and with two derivations, we have $-E'(-t)H(t)+E(-t)H'(t)=0$ and $E''(-t)H(t)-2E'(-t)H'(t)+E(-t)H''(t)=0$, so we can express β with H and its derivatives : $\beta(t)=(N^2-N)+2(N-1)\frac{tH'(t)}{H(t)}+2\frac{t^2H'^2(t)}{H^2(t)}-\frac{t^2H''(t)}{H(t)}$. Since $tH'(t)=H(t)(-N+S(t))$, γ can be expressed with H and its derivatives too, and we find the same expression, that proves that $\beta(t)=\gamma(t)$ and therefore $\beta_{k-1}=\gamma_{k-1}$. □

PROOF. We give now the proof of theorem 4. By lemma 1, $r_k=\sum_{i=1}^N z_i^k Z_i=\sum\frac{z_i^k Q''(z_i)}{2Q'(z_i)}=\sum\frac{F(z_i)}{Q'(z_i)}$ where $F(z)=\frac{z^kQ''(z)}{2}$. Writing $Q(z)=z^N-e_1z^{N-1}+e_2z^{N-2}+\cdots+(-1)^Ne_N$, we obtain $F(z)=\frac{1}{2}\sum_{j=0}^N(-1)^j(N-j)(N-j-1)e_jz^{N-j+k-2}$. Using linearity and lemma 2, we have exactly $2r_k=\sum_{j=0}^N(-1)^je_j(N-j)(N-j-1)h_{k-j-1}$. Using lemma 4, we obtain the theorem 4. □

4. FROM TWO BLOCKS TO SYMMETRIC FUNCTIONS IN ONE BLOCK

4.1 General case under the rational parameterization assumption

We return now to the general case where each U_i is an equation in $\mathbb{A}[\mathscr{Z},\bar{\mathscr{Z}}]$ where $\mathscr{Z}=\{z_1,\ldots,z_N\}$ and $\bar{\mathscr{Z}}=\{Z_1,\ldots,Z_N\}$; in addition, we require that the algebraic system fulfils the following parameterization assumption:

Definition 6 *We say that the system $U_i=0$ is under parameterization assumption if for all i, $Z_i=R(z_i)$ where $R(z)=\frac{N(z)}{M(z)}\in\mathbb{A}(z)$ with $\mathbb{A}=\mathbb{Q}(e_1,e_2,\ldots,e_N)$ an univariate rational function whose coefficients depend on the symmetric functions of the z_i.*

This hypothesis is well adapted to algebraic problems in the plane and more specifically to the vortex problem since lemma 1 can be reformulated:

Proposition 1 *The vortex problem satisfies the rational assumption since $Z_i=\frac{1}{2}\frac{Q''(z_i)}{Q'(z_i)}$ with $Q(z)=\prod_{i=1}^N(z-z_i)=z^N+e_2z^{N-2}+\cdots+(-1)^Ne_N$.*

For now, we assume that the system is under this assumption. We now describe an algorithm to obtain invariant equations under the action of $\mathfrak{S}_n$. First, we apply the algorithm ComputeInvariantSystem to compute the invariant equations V_i. Denote again by $Q(z)$ the polynomial $\prod_i(z-z_i)=z^N-e_1z^{N-1}+\cdots+(-1)^Ne_N$. There exist two polynomials B and C in $\mathbb{K}[e_1,\ldots,e_N][z]$ such that $BQ+CM=R_M$, where R_M is the resultant of Q and M with respect to the variable z. Then, $R_MZ_i=R_M\frac{N(z_i)}{M(z_i)}=N(z_i)C(z_i)$ since $Q(z_i)=0$. More generally, $R_M^kZ_i^k=(N^k\times C^k)(z_i)=(N^k\times C^k \bmod Q)(z_i)$ for all $k\geq 0$.

For each $W\in\{V_i,\bar{V}_i\}$, we substitute $\frac{1}{R_M^k}(N^k\times C^k \bmod Q)(z_i)$ to Z_i^k in each monomial of W. Up to a multiplication by an appropriate power of R_M^k to obtain polynomials, we obtain equations involving only the variables $z_1,\ldots,z_N$. These polynomials are invariant under $\mathfrak{S}_N$, and can be expressed as equations in the e_i.

These ideas give the following algorithm, we denote by $\partial_{\mathscr{Z}}P$ the total degree of P as polynomial of $\mathbb{A}[Z_1,\ldots,Z_N]$ with $\mathbb{A}=\mathbb{K}[z_1,\ldots,z_N]$. For all polynomial P in $\mathbb{K}[z_1,\ldots,z_N]^{\mathfrak{S}_N}$, let $\Sigma(P)$ be the expression of P as polynomial of $\mathbb{K}[e_1,\ldots,e_N]$.

ComputeSymmetricFunctionsSystem

Input: The invariant equations $V_i,\bar{V}_i$ of variables $\mathscr{Z}=\{z_1,\ldots,z_N\}$ and $\bar{\mathscr{Z}}=\{Z_1,\ldots,Z_N\}$

Output: A system of $2N$ equations of variables e_i, the symmetric functions of the z_i.

1. $m:=Max\{\partial_{\mathscr{Z}}W,\ ,W\in\{V_i,\bar{V}_i\}\}$; $\quad L_{NC}:=[(NC)^i \bmod Q, i\in 1..m]$;
2. for W **in** $\{V_i,\bar{V}_i,i=1..N\}$ **do**
  $d_W:=\partial_{\mathscr{Z}}(W)$;
  for U monomial of W **do**
    $d_U:=\partial_{\mathscr{Z}}(U)$;
    $Z_i^k\leftarrow L_{NC}[k](z_i)$ in U.
  end for.
  $U\leftarrow R_M^{d_W-d_U}U$ in W.
end for.
3. return $\{\Sigma(W)\}$

Example 3 *For the vortex problem, according to* (4)*, the denominator M is equal to Q', and the relation that we have is $BQ+CQ'=D$, where D is the discriminant of $Q(z)$ with respect to the variable z. Let $P_Z(z)$ be the polynomial of $\mathbb{K}[e_2,\ldots,e_N][z]$ equal to $\frac{1}{2}Q''C \mod Q$. Then, P_Z sends z_i on DZ_i, and we can apply the previous algorithm to compute symmetric equations. From $V_k=2r_k-\sum_{i=0}^{k-1}s_is_{k-1-i}+ks_{k-1}=0$, we obtain always 0, but not from $\bar{V}_k$. In this specific case, instead of using previous algorithm, there is a faster way to compute the equations, explained in the subsection hereafter.*

4.2 Invariant system of equations for the vortices problem

We introduce the two $\mathbb{K}[e_2\ldots,e_N]$-modules morphisms :

$$\begin{array}{rccc}\mathscr{S}: & \mathbb{K}[e_2,\ldots,e_N][z] & \longrightarrow & \mathbb{K}[e_2,\ldots,e_N]\\ & P(z)=\sum a_kz^k & \longmapsto & S(P)=\sum a_ks_k\end{array}$$

$$\begin{array}{rccc}\mathscr{H}: & \mathbb{K}[e_2,\ldots,e_N][z] & \longrightarrow & \mathbb{K}[e_2,\ldots,e_N]\\ & P(z)=\sum a_kz^k & \longmapsto & \sum a_kh_{k-N+1}\end{array}$$

Proposition 2 *For any polynomial P in $\mathbb{K}[e_2,\ldots,e_N][z]$ we have $\mathscr{S}(P)=\mathscr{S}(P \bmod Q)$ and $\mathscr{H}(P)=\mathscr{H}(P \bmod Q)$. Moreover*

$$\mathscr{S}(P)=\sum_{i=1}^N P(z_i)\quad\text{and}\quad\mathscr{H}(P)=\sum_{i=1}^N\frac{P(z_i)}{Q'(z_i)}$$

If $\deg(P)<N$ then $\mathscr{H}(P)=a_{N-1}$.

From theorem 4, we know that $2r_k=\sum_{i=0}^{k-1}s_is_{k-1-i}-ks_{k-1}$, therefore we have the conjugate equation:

$$2R_k=\sum_{i=0}^{k-1}S_iS_{k-1-i}-kS_{k-1}\tag{6}$$

One way to obtain directly symmetric equations is to compute:

$$S_k=\sum_{i=1}^N Z_i^k=\frac{1}{D^k}\sum_{i=1}^N P_Z^k(z_i)=\frac{1}{D^k}\mathscr{S}(P_Z^k(z)\mod Q)$$
$$R_k=\sum_{i=1}^N z_iZ_i^k=\frac{1}{D^k}\sum_{i=1}^N z_iP_Z^k(z_i)=\frac{1}{D^k}\mathscr{S}(zP_Z^k(z)\mod Q)$$

Substituting these expressions in (6) we obtain:

Proposition 3 *Given the Bézout relation $B(z)Q(z)+C(z)Q'(z)=D$, for any N and k, the solution of the vortex problem satisfies the following symmetric equations:*

$$2\frac{1}{D}\mathscr{S}(zP_Z^k)=\sum_{i=0}^{k-1}\mathscr{S}(P_Z^i)\mathscr{S}(P_Z^{k-1-i})-k\mathscr{S}(P_Z^{k-1})$$

where $\mathscr{S}(1) = N$ *and* $P_Z = \frac{1}{2}Q''C$.

The drawback of the method is that high powers of the discriminant occur in the resultant equations. Instead of using the polynomial P_Z to obtain equations with the e_i's, as explained in the previous section we will give a more efficient method using the $\mathscr{H}$ morphism.

Using the following lemma it is possible to compute R_k and S_k with powers of the discriminant divided by two:

Lemma 5 *Given the Bézout relation* $B(z)\,Q(z) + C(z)\,Q'(z) = D$, *we have*

$$D\,\frac{Q''}{Q'^2}(z_k) = A(z_k)$$

where $A(z)$ *is the polynomial* $-(B(z)+C'(z))$.

PROOF. By derivating the relation $B(z)\,Q(z) + C(z)\,Q'(z) = D$, we obtain $B'(z)Q(z) + (B'(z)+C(z))Q'(z) + C(z)Q''(z) = 0$. Modulo $Q(z)$, we have $-(B+C')Q' = CQ''$, so that $-(B+C')Q'C = -(B+C')D = CQ''$ where $A(z) = -(B(z)+C'(z))$. Modulo Q, we deduce that $A = \frac{Q''C^2}{D} = \frac{DQ''}{Q'^2}$. □

Hence, with one power of A, there are two powers of Q' in the denominator, and only one power of D in the numerator. If we use the morphism $\mathscr{H}$ when k is odd, we obtain R_k and S_k. More exactly:

Proposition 4 *The expressions of* S_i *and* R_i *in terms of the symmetric functions of the* z_i*'s are :*

$$\begin{array}{ll} D^k S_{2k} = \frac{1}{2^{2k}}\mathscr{S}(Q''^k A^k) & D^k R_{2k} = \frac{1}{2^{2k}}\mathscr{S}(zQ''^k A^k) \\ D^k S_{2k+1} = \frac{1}{2^{2k+1}}\mathscr{H}(Q''^{k+1} A^k) & D^k R_{2k+1} = \frac{1}{2^{2k+1}}\mathscr{H}(zQ''^{k+1} A^k) \end{array}$$

and all polynomials could be taken modulo Q.

Substituting these expressions in (6) we obtain:

Theorem 5 (Symmetric Equations) *Given the Bézout relation* $B(z)\,Q(z) + C(z)\,Q'(z) = D$, *for any N and k, the solution of the vortex problem satisfies the following symmetric equations:*

$$\begin{array}{c} \frac{1}{2D}\,\mathbf{S}_{2k+1} = \sum_{i=0}^{k-1} \mathbf{S}_{2i}\,\mathbf{H}_{2(k-i-1)} - 2k\,\mathbf{H}_{2k-2} \\ \mathbf{H}_{2k+1} = \sum_{i=0}^{k} \mathbf{S}_{2i}\,\mathbf{S}_{2(k-i)} + D\sum_{i=0}^{k-1} \mathbf{H}_{2i}\,\mathbf{H}_{2(k-i-1)} - (2k+1)\,\mathbf{S}_{2k} \end{array}$$

where $\mathbf{S}_{2i+\delta} = \mathscr{S}(z^\delta\, Q''^i A^i)$, $\mathbf{H}_{2i+\delta} = \mathscr{H}(z^\delta\, Q''^{i+1} A^i)$ *for* $\delta = 0, 1$ *and* $A(z)$ *is the polynomial* $-B(z) - C'(z)$.

PROOF. We substitute the expression of R_{2k}, R_{2k+1}, S_{2k}, S_{2k+1} given by proposition 4 into the equations:

$$\begin{array}{ll} 2R_{2k} & = 2\sum_{i=0}^{k-1} S_{2i}\,S_{2k-1-2i} - 2kS_{2k-1} \\ 2R_{2k+1} & = \sum_{i=0}^{k} S_{2i}\,S_{2k-2i} + \sum_{i=0}^{k-1} S_{2i+1}\,S_{2k-2i-1} - (2k+1)\,S_{2k} \end{array}$$

□

This theorem gives a very efficient algorithm to compute a system involving only the e_i, which solutions include all symmetric functions of the vortex problem. To simplify the description of the algorithm we introduce the following notation $\alpha_{i,k}$ and β_k, which depend only on the parity of i and k:

$$\beta_k = \left\{ \begin{array}{l} 0 \text{ if k is odd} \\ 1 \text{ if k is even} \end{array} \right. \qquad \alpha_{i,k} = \left\{ \begin{array}{l} 0 \text{ if i is even and k odd} \\ 1 \text{ otherwise} \end{array} \right.$$

ComputeSymmetricFunctionsVorticesSystem

Input: N, the polynomials Q, D and $A = -B - C'$, where B and C appear in the Bézout relation $BQ + CQ' = D$, and the two functions $\mathscr{S}$ and $\mathscr{H}$
Output: Symmetric polynomials in the e_i's.

1. $L_R := [\frac{N(N-1)}{2}]$; $L_S := [0]$; $P := 1$;
2. **for** $k = 2$ **to** $N-1$ **do**
  if IsOdd(k) **then**
    $L_S := L_S \cup [\mathscr{H}(\frac{1}{2}PQ'' \mod Q)]$;
    $L_R := L_R \cup [\mathscr{H}(\frac{z}{2}PQ' \bmod Q)]$;
  else
    $P := \frac{PAQ''}{4} \mod Q$;
    $L_S := L_S \cup [\mathscr{S}(P)]$;
    $L_R := L_R \cup [\mathscr{S}(zP \mod Q)]$;
  end if
end for
3. **return** $\{2L_R[k] - \sum_{i=1}^{k-2} D^{\alpha_{i,k}} L_S[i]\,L_S[k-1-i] - (2N-k)\,D^{\beta_k} L_S[k-1],\ k = 2 \ldots N-1\}$

Remark 5 *The equation* $2R_1 = N(N-1)$ *gives always* $0 = 0$. *We explain this fact in the next section.*

Example 4 *For* $N = 4$, $Q(z) = z^4 + e_2 z^2 - e_3 z + e_4$ *and it is easy to compute successively* $A(z) = (-8{e_2}^3 + 32 e_4 e_2 - 36 {e_3}^2)z^2 - 8e3(12e_4 + {e_2}^2)z - 54{e_3}^2 e_2 + 80 e_4 {e_2}^2 - 192 {e_4}^2 - 8{e_2}^4$. *From theorem 5 the first equation is* $R_2 = 0 = \mathscr{S}(zA(z)Q''(z))$. *Hence we compute* $P{=}zAQ'' \mod Q = (640 e_4 {e_2}^2 - 16{e_2}^4 - 2304 {e_4}^2 - 288 {e_3}^2 e_2)z^3 - 16 e_3 (27{e_3}^2 - 84 e_4 e_2 + {e_2}^3)z^2 + (-204 {e_3}^2 {e_2}^2 + 256 e_4 {e_2}^3 - 768 {e_4}^2 e_2 - 16{e_2}^5 - 720 e_4 {e_3}^2)z + 96 e_4 e_3 (12 e_4 + {e_2}^2)$. *The next step is to replace* z^3 *by* $s_3 = 3e_3$, z^2 *by* $s_2 = -2e_2$ *and* z *by* $p_1 = 0$ *so that* $0 = \mathscr{S}(zAQ'') = -16 e_3 (12 e_4 + {e_2}^2)^2$. *In the same way, we compute the second equation* $\mathscr{H}(zQ''^2 A) - (2N-3)\mathscr{S}(AQ'') = 0$. *We obtain the system of two equations:*

$$\left\{ \begin{array}{rcl} e_3(e_2^2 + 12e_4)^2 & = & 0 \\ e_2(e_2^4 - 16e_2^2 e_4 + 9e_2 e_3^2 + 48 e_4^2) & = & 0 \end{array} \right. \tag{7}$$

5. SOLVING THE EQUATIONS WITH THE SYMMETRIC FUNCTIONS

The goal of this section is to solve explicitly the symmetric equations by exact methods. To achieve this we use Gröbner bases computation.

5.1 The case $N = 4$

Interestingly enough, we can solve the vortex problem by hand when $N = 4$. Hence, we give the complete resolution of the case $N = 4$ without Gröbner Basis computation: The symmetric equations are given by (7) and, in addition, we assume that the discriminant $D = 16e_2^4 e_4 - 4e_2^3 e_3^2 - 128 e_2^2 e_4^2 + 144 e_2 e_3^2 e_4 - 27 e_3^4 + 256 e_4^3 \neq 0$, to ensures that the z_i's are distinct.

Lemma 6 *In equations* (7), *if* $e_2 \neq 0$, *then* $e_3 = 0$.

PROOF. We prove it by reduction to the absurd. If $e_2 \neq 0$ and $e_3 \neq 0$, the first equation gives $e_4 = -\frac{1}{12}e_2^2$, and the second equation becomes $8e_2^3 + 27e_3^2 = 0$, but $(8e_2^3 + 27e_3^2)^2$ is the discriminant of Q, up to a constant factor, which is a contradiction. □

Then, if $e_2 \neq 0$, $e_3 = 0$, and the second equation becomes $(e_2^2 - 12e_4)(e_2^2 - 4e_4) = 0$, but D becomes $16e_4(e_2^2 - 4e_4)^2 \neq 0$, so $e_4 = \frac{1}{12}e_2^2$. If $e_2 = 0$ then $e_3 = 0$ or $e_4 = 0$. We can conclude that:

Proposition 5 *When* $N = 4$, *there are three solutions to the vortex problem :*

$$Q(z) = z^4 + e_2 z^2 + \frac{1}{12}e_2^2 \qquad Q(x) = z^4 - e_3 z \qquad Q(x) = z^4 + e_4$$

The indetermination on e_2, e_3 or e_4 will be explained and solved in the next section as shown in the figures 1,2 and 3.

5.2 Homogeneity of the equations

Proposition 2 *The equation we obtained in the previous section are homogeneous for the degree* $d = \sum_k k \times \partial_{e_k}$, *where* ∂_{e_k} *is the degree in* e_k. *More exactly, the k-th equation has degree* $d = N(N-1)\lfloor \frac{k}{2} \rfloor + 1 - k$.

PROOF. We started from $2R_k = \sum S_i S_{k-1-i} - kS_{k-1}$. With $Z_i = \sum_{k \neq i} \frac{1}{z_i - z_k}$, we see that this equation is homogeneous in the z_i of degree $1-k$. The discriminant $D = \prod_{i \neq j}(z_i - z_j)$ is homogeneous of degree $2\binom{N}{2}$. So, the previous equation is homogeneous in the z_i with degree $2\lfloor \frac{k}{2} \rfloor \binom{N}{2} + 1 - k$. The symmetric function e_k is homogeneous in the z_i of degree k, that's why we took the degree d. □

Recall that we have lost the equation $2r_1 = 2R_1 = N(N-1)$, but there is no surprise : we have seen that the set of solutions (the z_i's) is invariant under multiplication by a complex of modulus one. This implies that the algebraic variety with variables $(e_2, \ldots, e_N)$ is invariant under the operation $(e_2, \ldots, e_N) \mapsto (\gamma^2 e_2, \ldots, \gamma^N e_N)$, with $|\gamma| = 1$. But an ideal associated to such a variety is homogeneous for the previous degree d : let P a polynomial in this ideal, and write $P = \sum_u P_u$, with P_u the homogenous part of degree u for the degree d, then if $(e_2, \ldots, e_N)$ is a zero of P; we have $\sum_u \gamma^u P_u(e_2, \ldots, e_N) = 0$ for all γ of modulus 1. A non-zero univariate polynomial have only a finite number of roots, so this polynomial (in γ) is null and $P_u(e_2, \ldots, e_N) = 0$ for all u. Another argument is that for $k = 1$, the degree of R_1 (in z_i) is zero, so we have to obtained from $2R_1 = N(N-1)$ an homogeneous equation of degree d equal to 0. There are solutions for all N to the vortex problem (see [2]), so this equation is 0.

5.3 Strategy to obtain a Gröbner Basis

Because of the homogeneity, we can suppose that any of the symmetric functions e_i is equal to 1 or 0. If it is 0, we have again an homogeneous system, so we can suppose that another symmetric function e_j is equal to 1 or 0, and so on. We have to add a new equation for being sure that all the z_i are distinct : $h \times D = 1$. (We can't solve it and remove the spurious solutions easily : for example, for $N = 5$, the system with $e_2 = 1$ without $h \times D = 1$ is 1-dimensional.)

According to the benchmark, it seems that the fastest way to compute a Gröbner Basis is to separate the system into two parts, $e_2 = 1$ or $e_2 = 0$ and compute a Gröbner Basis with DRL order with $h > e_N > \cdots > e_3$, and then perform a change of ordering from DRL to the lexicographic order with FGLM (see [9, 7]). For the component with $e_2 = 0$, we separate $e_3 = 1$ or $e_3 = 0$, and so on.

Then, we perform a Triangular Decomposition (see [15]) of each component.

Remark 6 *To compute a Gröbner Basis, we supposed that* $e_k = 1$ *for some k. But with this assumption, the solutions* $(z_1, \ldots, z_N)$ *that we obtain are not solutions of the equations* (E_i) $\quad \bar{z_i} = \sum_{j \neq i} \frac{1}{z_i - z_j}$ *but of* $\lambda \bar{z_i} = \sum_{j \neq i} \frac{1}{z_i - z_j}$ *for some* $\lambda > 0$. *Denote by* $(az_1, \ldots, az_N)$ *the solutions of* (E_i), *where a can be supposed to be a positive real. Then* $2r_1 = 2R_1 = 2a^2 \sum_i |z_i|^2 = N(N-1)$, *and* $a = \sqrt{\frac{N(N-1)}{2\sum |z_i|^2}}$. *The true value of* e_k *is* $\sum a z_{i_1} \times \cdots \times a z_{i_k} = a^k$.

Example 5 *With* e_2, e_3 *or* e_4 *equal to 1, the solutions* $(z_1, \ldots, z_4)$ *for* $N = 4$ *are drawn below :*

In the case of the four aligned points, $\sum_i |z_i|^2$ *is equal to 2, so we have to perform a multiplication by* $\sqrt{3}$ *to obtain the solutions of* (E_i). *In the case of the centered equilateral triangle,* $\sum_i |z_i|^2 = 3$, *so* $a = \sqrt{2}$ *and in the case of the square,* $\sum_i |z_i|^2 = 4$, *so* $a = \sqrt{\frac{3}{2}}$.

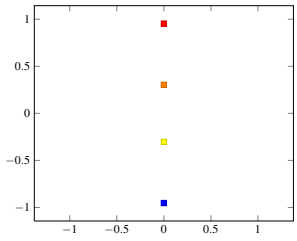

Figure 1: $Q(z) = z^4 + z^2 + \frac{1}{12}$

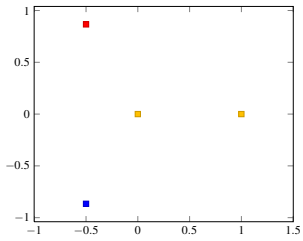

Figure 2: $Q(z) = z^4 - z$

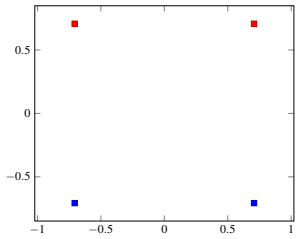

Figure 3: $Q(z) = z^4 + 1$

5.4 Removing spurious solutions

We can solve the system to obtain approximations of the e_i and then approximations of the z_i, but there are spurious solutions: we have to check that $P_Z(z_i) = D\bar{z_i}$ for each i to be sure that we have computed a true solution. Another way to perform it is to introduce two news variables x and z and add to the system the equations $P_Z(z) + Dz = x$ and $z^N + e_2 z^{N-2} + \cdots + (-1)^N e_N$, with P_Z the polynomial computed previously, which maps z_i to DZ_i. The next step is to perform a Gröbner elimination with lexicographical order $z > e_N > \cdots > e_k > x$ to obtain an univariate polynomial $P_{\Re}$ in x. Then we isolate the real roots of this polynomial $P_{\Re}$ using certificated methods.

5.5 Other symmetries

Suppose that we are in the component $e_2 = 1$, we have said that if $e_2, \ldots, e_N$ is a solution, then $\lambda^2 e_2, \ldots, \lambda^N e_N$ too, for all λ of modulus 1. If $\lambda = -1$ (geometrically, we do a symmetry of center O), e_2 stays at 1, but e_3 is changed to $-e_3$, so we can keep only half of the possible e_3. $(e_2, \ldots, e_N) \to (\bar{e_2}, \ldots, \bar{e_N})$ gives an other solution, so if e_3 is not real, we can suppose e_3 of imaginary part non negative. If e_3 is real and e_4 not, we can keep only the e_4 with imaginary part non negative, and so on.

5.6 Naive Approach

It is possible to solve directly the original system of $2N$ equations $(E_i, \bar{E_i})$ in z_i and Z_i. Because of invariance by multiplication by a scalar of modulus 1, we can suppose that z_1 is real, so we add the equation $z_1 = Z_1$. This trick will give an ideal of dimension 0, if we suppose that $z_1 \neq 0$. We will split the ideal into two parts : in the first one, we add the equation $z_1 \times \alpha = 1$, and in the second one, we add $z_1 = 0$, and we can add $z_2 = Z_2$. In each case, the ideal is zero dimensional, if we add the last equation $\prod_{i<j}(z_i - z_j)\beta = 1$, for being sure that all the z_i are distinct. We report in table 1 the following timings in Magma to compute the corresponding Gröbner basis (∞ means that we stopped the computation after five days):

It is possible to introduce the invariant ring of the subgroup of

	3	4	5
$\mathbb{Q}$	$0.02s$	$176.8s$	∞
$\mathbb{F}_{65521}$	$0.01s$	$0.2s$	∞

Table 1: Direct approach: Gröbner bases of the non symmetric systems with Magma.

$\mathfrak{S}_N \times \mathfrak{S}_N$, the elements of which are (σ, σ). We report in table 2 the number of secondary invariants in the Hironaka decomposition or the number of fundamental invariants over $\mathbb{Q}$, and the timings to compute them in Magma.

	3	4	5	6	7
Secondary Invariants	6	24	120	?	?
Timings	$0.0s$	$0.1s$	$225s$	∞	∞
Fundamental Invariants	9	14	20	27	?
Timings	$0.0s$	$0.1s$	$3.0s$	$400s$	∞

Table 2: Invariant Ring : Hironaka Decomposition and Fundamental Invariants with Magma.

5.7 Generating and solving the symmetric system

We have implemented the algorithm ComputeSymmetricFunctionsVorticesSystem in Maple and Magma to generate the symmetric system. We report in table 3 the timings to compute the systems depending only on the symmetric functions e_i using ComputeSymmetricFunctionsVorticesSystem algorithm with Magma (Intel Xeon 2.93 GHz with 128GB Ram).

	4	5	6	7	8
Magma	$0.0s$	$0.0s$	$0.06s$	$70.6s$	$7649.6s$
Maple	$0.0s$	$0.2s$	$0.9s$	$41.9s$	$2407.3s$

Table 3: Time to generate the symmetric systems with Maple or Magma.

On the same computer, the times to compute a Gröbner Basis using Magma of the symmetric system and perform a triangular decomposition of each component (mostly for the component with $e_2 = 1$) are presented in table 4.

When $N = 7$ we use FGb [13] to compute the corresponding Gröbner bases: it takes 144 sec to compute the system over $\mathbb{F}_{65521}$ and about 20 minutes to compute a Gröbner basis and a triangular decomposition over $\mathbb{Q}$. We postpone to section 7 the complete prime decomposition of the ideal corresponding to $N = 7$; using all the symmetries the problem admits 12 solutions; among them, 2 solutions are expressed as algebraic numbers of degree 82. For $N = 8$ the computation is still running but the most difficult part is already done (it takes 12 days to compute the first Gröbner basis). A web page was created to collect all the data: `http://www-salsa.lip6.fr/~jcf/vortices/`

	4	5	6	7
$\mathbb{Q}$	$0.02s$	$0.10s$	$296.7s$	?
$\mathbb{F}_{65521}$	$0.53s$	$1.58s$	$3.9s$	$1680.8s$

Table 4: Gröbner bases of the symmetric systems with Magma.

6. REFERENCES

[1] A. Albouy. The symmetric central configurations of four equal masses. *Contemporary Mathematics*, 198:131–135, 1996.

[2] H. Aref, P. K. Newton, M. A. Stremler, T. Tokieda, and D. L. Vainchtein. Vortex crystals. *Advances in Applied Mathematics*, 39, 2002.

[3] A. Colin. Solving a system of algebraic equations with symmetries. *J. Pure Appl. Algebra*, 117/118:195–215, 1997. Algorithms for algebra (Eindhoven, 1996).

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[5] T. Dirksen and H. Aref. Close pairs of relative equilibria for identical point vortices. *Phys. Fluids*, 23, 2011.

[6] J.-C. Faugère, M. Hering, and J. Phan. The membrane inclusions curvature equations. *Advances in Applied Mathematics*, 31(4):643–658, June 2003.

[7] J.-C. Faugère and C. Mou. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 115–122, New York, NY, USA, 2011. ACM.

[8] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 151–158, New York, NY, USA, 2009. ACM.

[9] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[10] G. Björck. Functions of modulus 1 on Zn , whose Fourier transforms have constant modulus, and "cyclic n-roots". *NATO, Adv. Sci. Inst. Ser. C, Math. Phys. Sci.*, 315:131–140, 1990. Recent Advances in Fourier Analysis and its applica tions.

[11] H. von Helmholtz. Über Integrale der hydrodynamischen Gleichungen, welche den Wirbelbewegungen entsprechen. *Reine Angew. Math.*, 55:25–55, 1858. English translation by Tait, P.G., 1867. On integrals of the hydrodynamical equations, which express vortex-motion. Philos. Mag. 33(4), 485–512.

[12] J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: a ring-based public key cryptosystem. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 267–288. Springer, Berlin, 1998.

[13] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In Komei Fukuda, Joris Hoeven, Michael Joswig, and Nobuki Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg.

[14] Lord Kelvin. On vortex atoms. *Proceedings of the Royal Society of Edinburgh*, VI:94–105, 1867. Reprinted in Phil. Mag. Vol. XXXIV, 1867, pp. 15-24.

[15] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Appl. Math.*, 33(1-3):147–160, 1991. Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[16] V.V. Meleshko and H. Aref. A bibliography of vortex dynamics 1858-1956. *Adv. Appl. Mech.*, 41(106), 2007.

[17] B. Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, second edition, 2008.

7. APPENDIX: SOLUTIONS FOR N=7

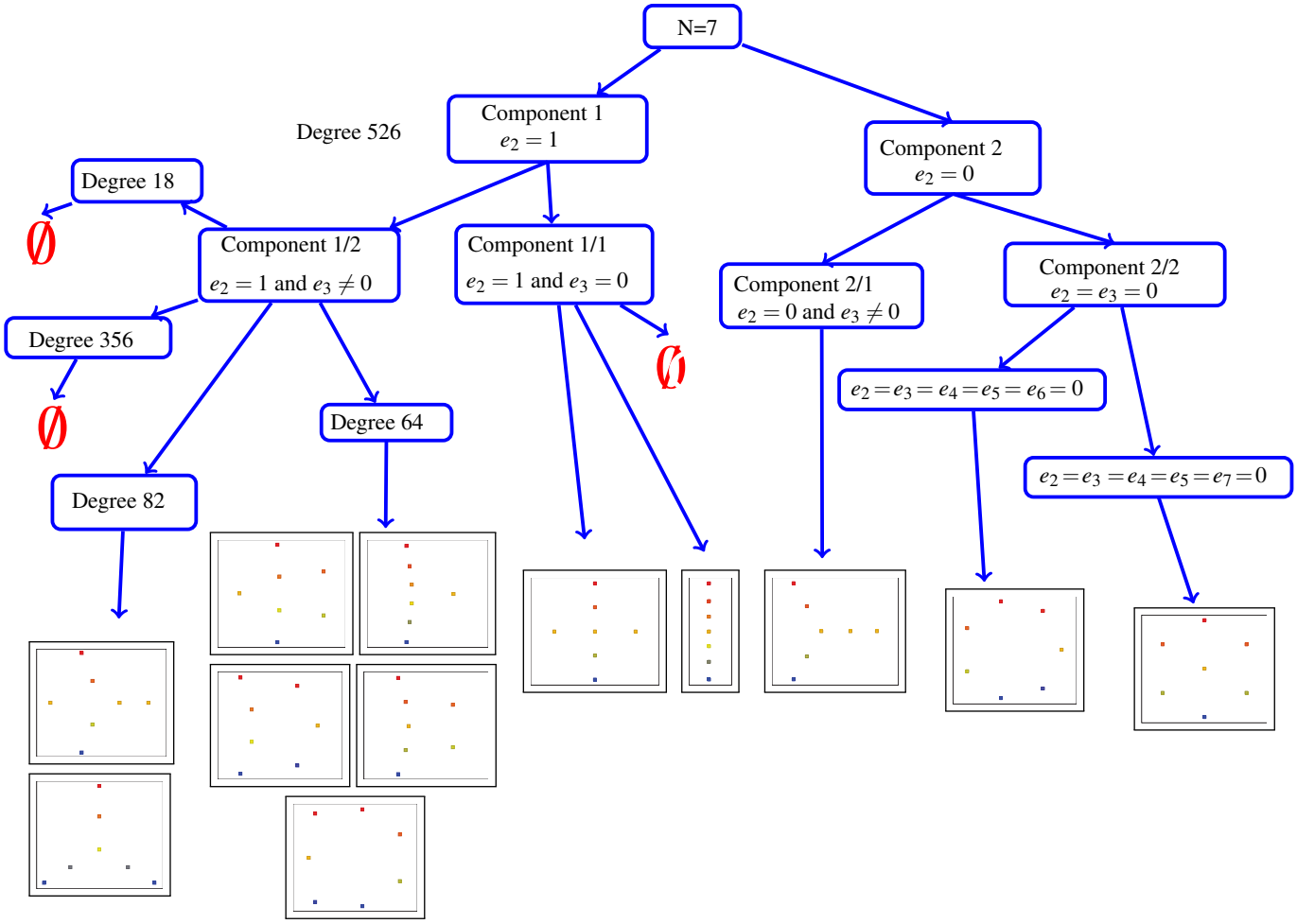

Figure 4: All the solutions of the vortex problem when $N = 7$